ATTACHMENT 4

TO

FA8807-05-C-0013

CONTRACT SECURITY CLASSIFICATION SPECIFICATION (DD254)

FOR NAVSTAR

GLOBAL POSITIONING SYSTEM (GPS)

GPS III OCX PRDA

11 July 2005

DEPARTMENT OF DEFENSE

CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED: SECRET

b. LEVEL OF SAFEGUARDING REQUIRED: SECRET

2. THIS SPECIFICATION IS FOR: (X and complete as applicable)

X	a. PRIME CONTRACT NUMBER: FA8807-05-C-0013	
	b. SUBCONTRACT NUMBER	
	c. SOLICITATION OR OTHER NUMBER	Due Date (*YYMMDD*)

3. THIS SPECIFICATION IS: (X and complete as applicable)

X	a. ORIGINAL (Complete date in all cases)		Date (*YYMMDD*): 20050708
	b. REVISED (Supersedes all previous specs)	Revision No.	Date (*YYMMDD*)
	c. FINAL (Complete item 5 in all cases)		Date (*YYMMDD*)

4. IS THIS A FOLLOW-ON CONTRACT? YES [ ] NO [X] If Yes, complete the following:

Classified material received or generated under _____ (*Preceding Contract Number*) is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254? YES [X] NO [ ] If Yes, complete the following:

In Response to the contractor's request dated 20050708, retention of the identified classified material is authorized for the period of 2 YEARS

6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)

a. NAME, ADDRESS, AND ZIP CODE	B. CAGE CODE	C. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)
Raytheon Company 16800 E Centre Tech Parkway Aurora, CO 80011-9046	5R497	Defense Security Service 12567 W Cedar Drive #150 Lakewood, CO 80228-2009

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	B. CAGE CODE	C. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)

8. ACTUAL PERFORMANCE

a. NAME, ADDRESS, AND ZIP CODE	B. CAGE CODE	C. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)
Raytheon Company 16800 E Centre Tech Parkway Aurora, CO 80011-9046	5R497	Defense Security Service 12567 W Cedar Drive #150 Lakewood, CO 80228-2009

9. GENERAL IDENTIFICATION OF THE PROCUREMENT

GPS III OCX PRDA: The contractor will develop a conceptual but innovative control segment architecture that addresses requirements in the DSS and those outlined in the CSOW and perform any optional test demonstrations for two or more of the following areas: a) Tracking, Telemetry & Control (TT&C), b) Navigation Mission, and c) Mission Planning.

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	X		a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		X
b. RESTRICTED DATA		X	b. RECEIVE CLASSIFIED DOCUMENTS ONLY		X
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	X	
d. FORMERLY RESTRICTED DATA		X	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	X	
e. INTELLIGENCE INFORMATION:			e. PERFORM SERVICES ONLY		X
(1) Sensitive Compartmented Information (SCI)		X	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X
(2) Non-SCI	X		g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	X	
f. SPECIAL ACCESS INFORMATION		X	h. REQUIRE A COMSEC ACCOUNT	X	
g. NATO INFORMATION		X	I. HAVE TEMPEST REQUIREMENTS		X
h. FOREIGN GOVERNMENT INFORMATION		X	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	X	
I. LIMITED DISSEMINATION INFORMATION		X	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		X
j. FOR OFFICIAL USE ONLY INFORMATION	X		l. OTHER (Specify)		X

k. OTHER (Specify)		X			

DD FORM 254, DEC 1999 Previous editions are obsolete

For Official Use Only

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release

[ ] Direct [X] Through (Specify):

SMC/PAS,
2430 E. El Segundo Blvd., Suite 4049
El Segundo, CA 90245-4687

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. Security Guidance. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes: to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

See Attached

The contractor shall protect IAW DoD D 5220.22-M National Industrial Security Program Operations Manual (NISPOM), CDRL A005 (PPIP) and as prescribed in applicable security classification guides.

//signed//
John J. Longwell, GG-13
Chief, ISPM Operations
SMC/AXP

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements identify the pertinent contracted clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.) [X] Yes [ ] No

See Attached

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use item 13 if additional space is needed.) [ ] Yes [X] No

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE (Include Area Code)
Carol A. Laechelt, GS-13	Procuring Contracting Officer	(310) 363-2788

d. ADDRESS (Include Zip Code)	17. REQUIRED DISTRIBUTION	
SMC/GPK	X	a. CONTRACTOR
2420 Vela Way, Suite 1866	X	b. SUBCONTRACTOR
El Segundo, CA 90245-4659	X	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
e. SIGNATURE		d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
//signed//	X	e. ADMINISTRATIVE CONTRACTING OFFICER
	X	f. OTHERS AS NECESSARY **SEA OOG, SMC/AXP, SMC/GPES-PPO**

DD FORM 254 (BACK), DEC 1999

Unclassified

ITEM 10a, 11h: Communications Security (COMSEC)

1. The Contractor is authorized access to COMSEC information and will comply with NSA Manual 90-1. Access to COMSEC material/information is restricted to U.S. citizens who have been briefed according to the NISPOM and possess an approved government clearance. NOTE: The COMSEC/CRYPTO briefing applies only to the use and control of CRYPTO equipment and specialized COMSEC publications.

2. NACSIM/NACSEM documents are not considered COMSEC controlled material. Additionally, cryptographic information/equipment shall be retained in a Contractor facility COMSEC account.

Reference Block 10e(2): Non-SCI

Provisions for the handling of Non-SCI or "Collateral" Intelligence by contractors is governed by Chapter 9, Section 3 of DoD 5220.22-M, the National Industrial Security Program Operating Manual, 1995 (NISPOM). Particular emphasis is placed on the contractor(s) correctly understanding and heeding intelligence portion markings. As classified material, collateral intelligence will be afforded the same protections, safeguards and precautions required by any classified material unless special intelligence related handling instructions are additionally imposed. These basic safeguards are found in DoD 5200.1-R, Information Security Program and AFI 31-401, Information Security Program Management. The disclosure or release of intelligence derived information, whether its status is collateral or SCI, is not authorized without the prior consent of SMC/IN.

Reference Block 10j: For Official Use Only (FOUO) Handling Instructions

FOR OFFICIAL USE ONLY (FOUO) information will be handled as follows:

1.0 General.

1.1 For Official Use Only (FOUO) is official government information that does not meet requirements for classification but still requires protection. By definition, information shall be unclassified in order to be designated FOUO. If an item of classified information is declassified, it may be designated FOUO if it qualifies under one of the other exemptions of the FOIA. This means that:

1.1.1 Information cannot be classified and FOUO at the same time. Therefore, classified documents containing FOUO information cannot bear an overall document marking of FOUO. However, portions or pages of a classified document, that contain only FOUO information will be marked as FOUO.

1.1.2 Information that is declassified may be designated FOUO, only if it is believed to fit into one or more of the last eight exemptions (exemptions 2 through 9).

1.2 FOUO information may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act (5 USC 552). Most FOUO information generated or handled in support of this contract will be exempt from mandatory disclosure under exemptions 4 and 5.

1.3 FOUO information may be released to the public; however, the Government prior to its release must review it. Information in support of this contract must be reviewed by SMC/PA prior to release.

2.0 Identification Markings.

2.1 An unclassified document containing FOUO information will be marked "FOR OFFICIAL USE ONLY" on the outside of the front cover (if any), on the first page, on each page containing FOUO information, on the back page, and on the outside back cover (if any). For convenience, all pages, even those that do not contain FOUO information may be marked in documents generated by automated systems.

2.2 Portion Marking FOUO Information. Subjects, titles and each section, part, paragraph, and similar portion of an FOUO document shall be marked to show that they contain information requiring protection. Use the parenthetical notation "(FOUO)" to identify information as For Official Use Only for this purpose. Place this notation immediately before the text.

2.3 Individual pages within a classified document that contain both FOUO and classified information will be marked top and bottom with the highest security classification of information appearing on the page. Individual portions/paragraphs containing FOUO information but no classified information will be marked "FOUO."

2.4 Marking information FOUO does not automatically qualify it for exemption. If a request for a record is received, the information shall be reviewed to determine if it actually qualifies for exemption. Similarly, the absence of the FOUO marking does not automatically mean the information shall be released. Some types of records (for example, personnel records) are not normally marked FOUO, but may still be withheld under the FOIA. All DoD unclassified information must be reviewed before it is released to the public or to foreign governments and international organizations.

2.4.1 The cover or the first page of unclassified documents containing FOUO information will be marked with the following statement:

This Document contains information EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FOIA. EXEMPTIONS (b)(4) and (b)(5) apply.

2.5 Certain classified material on this contract may be downgraded by the Original Classification Authority to FOUO or may be automatically declassified under E.O. 12958 as

Amended. When classified material approved for declassification to FOUO is used, extracted, reissued, transmitted and/or updated, it must be reviewed and appropriately marked.

3.0 Access to FOUO Information.

3.1 No person may have access to information designated as FOUO unless that person has been determined to have a valid need for such access in connection with the accomplishment of a lawful and authorized Government purpose.

3.2 The final responsibility for determining whether an individual has a valid need for access to information designated as FOUO rests with the individual who has authorized possession, knowledge or control of the information and not on the prospective recipient.

3.3 Information designated as FOUO may be disseminated within the DoD Components and between officials of DoD Components and DoD contractors, consultants, and grantees to conduct official business for the Department of Defense, provided that dissemination is not further controlled by a Distribution Statement.

3.4 DoD holders of information designated as FOUO are authorized to convey such information to officials in other Departments and Agencies of the Executive and Judicial Branches to fulfill a government function. If the information is covered by the Privacy Act, disclosure is only authorized if the requirements of DoD 5400.11-R are satisfied.

3.5 Release of FOUO information to Congress is governed by DoD Directive 5400.4. If the information is covered by the Privacy Act, disclosure is authorized if the requirements of DoD 5400.11-R are also satisfied.

3.6 DoD Directive 7650.1 governs release of FOUO information to the General Accounting Office (GAO). If the information is covered by the Privacy Act, disclosure is authorized if the requirements of DoD 5400.11-R are also satisfied.

4.0 Transmission/Dissemination/Reproduction.

4.1 Authorized contractors, consultants, and grantees may transmit/disseminate FOUO information internally to each other and to DoD components and officials of DoD components who have a legitimate need for the information in connection with this contract. The following guides apply:

4.1.1 FOUO information may be discussed over non-secure telephones and other electronic instruments. Cordless, cellular and mobile telephones should be avoided.

4.1.2 FOUO information may be transmitted over non-secure facsimile equipment.

4.1.3 Documents of facsimile transmissions containing FOUO material or with FOUO material attached must be marked to identify any FOUO contents or attachments.

4.1.4 FOUO information and material may be transmitted via first class mail, parcel post or, for bulk shipments, via fourth class mail. Electronic transmission of FOUO information, e.g., voice, data or facsimile, e-mail, shall be by approved secure communications systems or systems utilizing other protective measures such as Public Key Infrastructure (PKI), whenever practical.

4.1.4.1 FOUO information may be transmitted, processed, and stored on Automated Information Systems (AIS), electronic mail, and other similar systems or networks (1) when distribution is to an authorized recipient and (2) if the receiving system is protected by either physical isolation or a password protection system. Holders will not use general, broadcast, or universal mail addresses to distribute FOUO information. Discretionary access control measures may be used to preclude access to FOUO files by users who are authorized system users but are not authorized for FOUO information.

4.1.4.2 FOUO information may only be posted to DoD Web sites consistent with security and access requirements specified in Deputy Secretary of Defense Memorandum dated December 1998, Subject: "Web Site Administration".

4.1.5 Reproduction of FOUO information may be accomplished on unclassified copiers or within designated government or contractor reproduction areas.

5.0 Protection of FOUO Information.

5.1 During working hours, reasonable steps shall be taken to minimize risk of access by unauthorized personnel. After working hours, store FOUO information in unlocked containers, desks or cabinets if Government or Government-contract building security is provided. If such building security is not provided, store the information in locked desks, file cabinets, bookcases, locked rooms, etc.

6.0 Disposition.

6.1 Record copies of FOUO documents shall be disposed of according to the Federal Records Act and the DoD Component records management directives. Non-record FOUO documents may be destroyed by any of the means approved for the destruction of classified information, or by any other means that would make it difficult to recognize or reconstruct the information, e.g. by shredding and placing in a recycle or trash container or by initializing, degaussing, or shredding magnetic media.

6.2 FOUO material may be recycled. Safeguard the FOUO documents or information until recycled. Recycling contracts must include on how to protect and destroy FOUO material.

6.3 Removal of the FOUO status can only be accomplished by the government originator of the information. SMC/PA will review and/or coordinate the removal of FOUO status for SMC information in support of this contract.

7.0 Unauthorized Disclosure.

7.1 The unauthorized disclosure of FOUO does not constitute an unauthorized disclosure of DoD information classified for security purposes. However, appropriate administrative action shall be taken to fix responsibility for unauthorized disclosure of FOUO whenever feasible, and appropriate disciplinary action shall be taken against those responsible. Unauthorized disclosure of FOUO information that is protected by the Privacy Act may also result in civil and criminal sanctions against responsible persons. The Military Department or other DoD Component that originated the FOUO information, i.e. the contracting officer, shall be informed of its unauthorized disclosure.

Reference Block 11d: Fabricate, Modify, or Store Classified Hardware

The Contractor is required to provide adequate storage to the level of Secret for classified hardware that, due to size or quantity, cannot otherwise be safeguarded in GSA approved storage containers.

Reference Block 11g: Be Authorized to Use the Services of Defense Technical Information (DTIC) or Other Secondary Distribution Center

The contractor may access information provided by DTIC by complying with all established safeguards and following the registration procedures as set forth in Chapter 11 Section 2 of the NISPOM (DoD 5220.22M).

Reference Block 11j: OPSEC

Contractor will comply with all Program Protection Plans/System Protection Guides specified in the applicable Delivery Order Statement of Work or the DD Form 254. The contractor will accomplish the following minimum requirements in support of the User Agency Operations Security (OPSEC) Program and protect OPSEC Critical Information. Items of Critical Information are those facts which individually, or in the aggregate reveal sensitive details about SMC programs and contractor operations, and thus require protection from adversarial collection or exploitation.

Protect Critical Information and activities which could compromise classified information or operations, or degrade the planning and execution of military operations performed by the contractor in support of the mission. Such information may be marked FOR OFFICIAL USE ONLY, Privacy Act of 1974, COMPANY PROPRIETARY, Export Controlled, or otherwise designated as sensitive by the Special Program Office or SMC/AXP (OPSEC Manager).

Review items on the critical information list (CIL) as contained within the SMC OPSEC Plan and determine applicable to contractor operations. Include OPSEC as a part of the contracts ongoing security awareness program conducted in accordance with Chapter 3, Section 1, of the NISPOM or Chapter 3 of AFI 10-1101, as applicable. Be responsive to the User Agency OPSEC Manager (SMC/AXP) on a non-interference basis.

ITEM 14: Additional Security Requirements

Notification of Government Security Activity Required

Additional Distribution: SMC/INS, SMC/AXP

Project Office:

SMC/GPG
2420 Vela Way, Suite 1866
El Segundo, CA 90245-4659

Location(s) of Actual Performance: see block 8

Number of SCI Billets required while performing this contract: 0

Contract award limitations are as follow: 1) Prime Contractors must be U.S.-Owned, operated, and on-shore companies. 2) Sub-contractors are authorized to be offshore, foreign owned companies; however, they may only participate in Non-Restricted portions of the contract. The contractor will comply with NISPOM requirements.

NDS information, information up-to SECRET, received and generated during this procurement is not approved for public release and shall be safeguarded accordingly.

Reference protection and security documents undergo changes; these changes may significantly alter both contractor and government security support requirements.

Protection of classified information contained in the above reference documentation is considered paramount. The U.S. Government shall only authorize the dissemination of COMSEC information.

Establishment of Control Markings Authorized for GPS COMSEC information:
Special handling control markings have been identified by the Navstar GPS Joint Program Office and are annotated in appropriate section of the above referenced documents. These markings are defined for use only with appropriate classified and unclassified GPS COMSEC Information.

These markings shall be affixed to all GPS COMSEC information extracted from the appropriate referenced documents and used by the contractor. Specific requirements associated with access and handling of this information is defined below.

Protection of Control Markings:
The control markings standing alone are For Official Use Only and shall be protected in accordance with the FOUO handling instructions attached to this DD-254.

Access and Security:

a. Access authority: The U.S. Government shall grant Access authority to the classified references.

b. Briefing/debriefing requirements: The Navstar GPS JPO will do Briefing and debriefings. The contractor will submit in writing request for access to the PCO for access. Adequate information shall be provided to assist the government in approving access based upon sufficient clearance, need-to-know, and identification as defined in the NISPOM documents.

c. Establishment of Access Records: the GPS-III security manager for the government shall maintain a listing of all personnel holding the subject material provided by the contractor. Changes to the access list shall be made available to the government 5 working days after the government has approved the change.

Special Handling Protection:
a. Page Markings: Each page of a document containing GPS COMSEC information, information up-to the classification of SECRET shall be marked on the top and bottom with control markings discussed in this attachment.

e. Required Special Statement: The following statement shall also be affixed to the bottom of each page containing GPS COMSEC information:

COMSEC MATERIAL – ACCESS RESTRICTED TO U.S. CITIZENS HOLDING FINAL GOVERNMENT CLEARANCES

f. Cover Markings: In accordance with Navstar GPS COMSEC requirements and the Arms Export Control Act, as implemented by the International Traffic in Arms Regulation, the following statements shall be affixed to the cover of a document containing GPS COMSEC information:

COMSEC MATERIAL
ACCESS RESTRICTED TO U.S. CITIZENS HOLIDNG FINAL GOVERNMENT CLERANCES
-- NOT RELEASEABLE TO FOREIGN NATIONALS –

WARNING

This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, USC 2751 et esq.) or the Export Administration Act of 1979, as amended, Title 50, USC, App. 2401, et esq. Violation of these export-control laws are subject to sever criminal penalties. Dissemination of this document is controlled under DoD Directive 5230.25

Distribution F

Further dissemination only as directed by the Navstar GPS Joint Program Office (JPO) SMC/GP

This document may not be distributed in whole or in part, without the prior approval of the Navstar GPS JPO. This material is not releasable to the Defense Technical Information Center (DTIC) per DoD Instruction 5100.38

DESTRUCTION NOTICE

For classified documentation, follow the procedures in DoD 5220.22-M National Industrial Security Operating Manual, Chapter 5, and DoD 5200.1-R Information Security Program Chapter IX. For UNCLASSIFIED limited documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document

g. Transmission of classified GPS COMSEC information: Classified GPS COMSEC information and material controlled within the COMSEC Material Control System (CMCS) (ALC1-3 items) will only be transmitted via the Defense Courier Service (DCS). Use of USPS registered mail or USPS overnight express mail is permitted for up-to SECRET COMSEC material not controlled within CMCS. NOTE: items shipped through USPS must not be left within the system over weekends or holidays. All shipments should be sent Monday through Thursday during normal workweeks to prevent undue control limitation.